Exhibit E

1. Section 311 of the USA PATRIOT Act (31 U.S.C. § 5318A)

a. Prevented Act

Section 311 empowers federal regulators to require heightened "special measures" against financial institutions if their transactions could facilitate money laundering or terrorist financing. Financial institutions (broadly defined) must track, record, and disclose transaction data to ensure criminal or terrorist entities cannot easily move illicit funds.

b. Pump.Fun Violation

Pump.Fun fails to meet these strict requirements and **allows** fully anonymous creation, trading, and transfer of tokens, thereby inviting criminal abuse with virtually no oversight.

- **Fact 1**: **No Identity Verification**
  - **TOS Reference**: Pump.Fun's Terms of Service ("TOS") § 2 (Eligibility) does **not** require users to submit any identity documentation or verify themselves beyond a simple wallet connection.
  - **Specific Violation**: By not collecting user identities, Pump.Fun **cannot** comply with Section 311 mandates to track suspicious users or freeze suspect activity.
- **Fact 2**: **Anonymous Token Issuance**
  - **TOS Reference**: TOS § 1.1 indicates the platform is "designed to assist with the creation and trading of Digital Assets," but does **not** impose Know Your Customer ("KYC") obligations for creating these assets.
  - **Specific Violation**: Anyone can deploy a new memecoin, raising significant risk that criminals or terrorists will mint tokens, layer illicit funds, and cash out "clean" proceeds.
- **Fact 3**: **Inadequate Eligibility Checks**
  - **TOS Reference**: TOS § 2.1 outlines basic "eligibility" criteria but only mentions geographic restrictions and Pump's "sole discretion" to restrict usage. There is **no** mention of background checks or ID verification.
  - **Specific Violation**: Pump.Fun's entire user base remains effectively unverified, enabling potential infiltration by sanctioned entities or terror groups that exploit anonymity.

c. Real-World Consequences

Without compliance measures under Section 311, Pump.Fun becomes a magnet for **terrorist financing**, **drug trafficking**, and **other transnational crimes**. Criminals can launder money by

creating tokens, pumping trading volume, and selling them—effectively obscuring the source of their funds.

---

2. Bank Secrecy Act (BSA) / FinCEN Regulations (31 CFR § 1022)

a. Prevented Act

The BSA requires money services businesses ("MSBs") to implement a **written Anti-Money Laundering ("AML") program**, conduct risk-based customer due diligence, and file regulatory reports (e.g., Suspicious Activity Reports, Currency Transaction Reports). These obligations are intended to deter money laundering and flag illegal transactions.

b. Pump.Fun Violation

Pump.Fun does **not** maintain or disclose a meaningful AML compliance framework.

- **Fact 1**: **No Documented AML Policy**
  - **TOS Reference**: The TOS includes disclaimers about user conduct (§ 3.2, § 3.3) but **no** specific mention of an AML policy, Customer Identification Program ("CIP"), or compliance officers.
  - **Specific Violation**: Under 31 CFR § 1022.210, MSBs must have a **written AML program**. Pump.Fun's TOS offers no detail on **any** AML program.
- **Fact 2**: **Failure to Collect or Retain KYC Data**
  - **TOS Reference**: While § 5 states "We keep your personal data ... as may be required by law such as ... compliance with anti-money laundering laws," there is **no** actual process in place requiring users to submit personal data.
  - **Specific Violation**: Because Pump.Fun never requests IDs or documentation, there is no possibility of verifying or reporting suspicious customer activity as mandated by 31 CFR § 1022.210(d).
- **Fact 3**: **Inability to Monitor Transactions**
  - **TOS Reference**: TOS § 9.1 warns that Pump.Fun "does not represent or warrant that any actions by you ... will be completed successfully," but does **not** mention any internal transaction-monitoring system.
  - **Specific Violation**: FinCEN guidance requires ongoing monitoring to detect suspicious patterns. Pump.Fun cannot fulfill this if it lacks even the basic data to analyze user activity.

c. Resulting Illicit Pathways

- Criminal organizations can quickly move large sums of cryptocurrency, **launder** them through memecoin trades, and **withdraw** with no detection.
- **Human traffickers** and **child exploitation** rings exploit this oversight-free environment to covertly move proceeds.

---

3. Suspicious Activity Reports (SARs) & Currency Transaction Reports (CTRs)

a. Prevented Act

Under 31 CFR § 1022.320, MSBs must file SARs when transactions exceed certain thresholds or show red flags indicative of money laundering/terrorist financing. Additionally, 31 CFR § 1010.311 requires filing CTRs for transactions exceeding $10,000 (or crypto equivalent).

b. Pump.Fun Violation

Pump.Fun's TOS reveals **no** procedure to detect or report suspicious transactions nor to file CTRs for large cash-equivalent amounts.

- **Fact 1**: **No Threshold Triggers**
  - **TOS Reference**: Nowhere in §§ 4 (Fees and Calculations), 5 (Records), or 7 (Transactions) is there mention of threshold-based transaction oversight or reporting.
  - **Specific Violation**: By ignoring large transactions entirely, Pump.Fun fails to file **CTRs**.
- **Fact 2**: **No SAR Filing Process**
  - **TOS Reference**: TOS § 5 suggests they keep "records" but provides **no** step-by-step protocol for investigating or flagging irregular activity for SARs.
  - **Specific Violation**: Federal law mandates that suspicious activities—such as rapid buying/selling of tokens in large sums—be flagged and reported to FinCEN. Pump.Fun's TOS has no mechanism for such compliance.

c. Consequences

Organized criminals can exploit Pump.Fun to move over $10,000 daily in tokens—without raising any internal alarm—thus **circumventing** the BSA's critical reporting obligations and avoiding law enforcement scrutiny.

---

4. Office of Foreign Assets Control (OFAC) Sanctions Compliance

a. Prevented Act

All U.S. persons and businesses must screen customers against OFAC sanctions lists (e.g., Specially Designated Nationals ("SDNs"). This includes verifying user identities and blocking any individual or entity found on sanctions lists.

b. Pump.Fun Violation

Pump.Fun does **not** appear to conduct any sanctions screening.

- **Fact 1**: **No OFAC Mention**
  - **TOS Reference**: The only mention of banned jurisdictions is TOS § 2.1(c)(ii) referencing a "List of Prohibited Countries." However, **no** user identity checks exist to confirm someone's nationality/residency.
  - **Specific Violation**: Because Pump.Fun never obtains user information, it **cannot** run them against OFAC's SDN list. This directly violates OFAC compliance mandates.
- **Fact 2**: **Evasive Use of Wallets**
  - **TOS Reference**: TOS § 6.1 states users must connect a wallet but places **no** geographic or identity restrictions on that wallet.
  - **Specific Violation**: A sanctioned person from a "Prohibited Country" can trivially bypass Pump.Fun's vague ban by connecting a standard crypto wallet from any location, thereby **circumventing** sanctions altogether.

c. Hypothetical Example

A known Iranian terrorist financier, subject to U.S. sanctions, could connect a wallet to Pump.Fun, purchase large sums of tokens, and move funds internationally—**unimpeded**—because the platform never verifies user identity or location.

---

5. Failure to Obtain State Money Transmitter Licenses

a. Prevented Act

Many U.S. states require entities that transmit or facilitate transfers of money (including convertible virtual currencies) to obtain a **money transmitter license**. Licensees must meet bonding requirements, financial reporting rules, and AML standards.

b. Pump.Fun Violation

Nothing in the TOS indicates Pump.Fun has obtained the necessary state-level licenses.

- **Fact 1**: **No Mention of State Licensure**
  - **TOS Reference**: The TOS does not reference any money transmitter licensing or compliance with state banking regulations; Pump.Fun simply states it can restrict usage "at our absolute discretion" (TOS § 3.1).
  - **Specific Violation**: Operating as a de facto exchange for countless tokens meets most definitions of money transmission in multiple states. Absence of licensure is a direct breach of state laws.
- **Fact 2**: **Uniform Fees and Custody**
  - **TOS Reference**: TOS §§ 4.1-4.3 detail a fee structure and authorize Pump.Fun to deduct fees from user wallets.
  - **Specific Violation**: Handling user funds/fees triggers licensure requirements in states where the definition of "money transmission" includes exchanging or storing cryptocurrency. Pump.Fun does **not** appear to comply.

c. Resulting Liabilities

Pump.Fun's unlicensed operation may lead to **cease-and-desist** orders, hefty fines, or criminal penalties. Users have **no** state-level protections or recourse if fraud or platform insolvency occurs.

---

6. Specific Violations Under Pump.Fun's Own Terms of Service

While Pump.Fun's TOS acknowledges data collection "for compliance with anti-money laundering laws" (§ 5), the document provides **no** workable procedures, no CIP requirements, and **no** process for verifying user identity. The TOS disclaimers (e.g., "We are not your broker ... No fiduciary duty ... We do not recommend any Digital Asset ...") do **not** absolve Pump.Fun

from legal obligations to implement AML/KYC measures if it qualifies as a money transmitter or falls under federal and state securities or financial regulations.

---

7. Risks and Public Harm

- **Terrorist Financing**: Anonymous accounts allow extremist groups to move funds across borders unmonitored.
- **Drug Cartels / Human Trafficking**: Criminal organizations launder millions through memecoins, layering transactions to obscure illicit proceeds.
- **Proliferation of Scams**: Pump.Fun's easy issuance of tokens fosters rapid creation of fraudulent or "rug pull" coins, further harming unsuspecting investors.

Conclusion

Despite disclaimers in its Terms of Service, Pump.Fun is operating in **clear violation** of multiple U.S. financial crime prevention statutes and regulations, including Section 311 of the USA PATRIOT Act, the Bank Secrecy Act, FinCEN rules on SARs/CTRs, OFAC sanctions rules, and state money transmitter licensing requirements. By refusing to verify user identities, failing to monitor or report suspicious transactions, and neglecting any formal AML program, Pump.Fun exposes the public to **severe** risks of criminal exploitation—facilitating money laundering, terrorist financing, sex trafficking, and other serious crimes.